CLAIMS

1. A method for delivering certificates with associated trust information from a trust information provider to a client for verification of a received certificate by said client, comprising the steps of:

providing a trust information object (TIO) to said client; and

providing as part of said TIO a hash value of a trust entity certificate and associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate.

2. The method of Claim 1, wherein said TIO comprises any of:

a trusted entity's certificate;

a trust vector of said trusted entity's certificate;

a value indicating a number of signatures required for a next update;

a date said TIO is created; and

a digital signature of all data including said certificate, trust vector, number of signatures, and timestamp, contained in said TIO.

3. The method of Claim 1 wherein said hash value is determined using any of MD5 and SHA-1.

4. The method of Claim 1, said TIO conforming to the PKCS#7 standard.

5. The method of Claim 1, further comprising the step of:

hard coding a TIO derived from a set of popular root CA certificates into said client's software.

6. The method of Claim 1, further comprising the step of:

saving a copy of said TIO in a persistent memory during said client's build time.

7. A method for delivering certificates with associated trust information from a server to a client for verification of a received certificate by said client, comprising the steps of:

associating a trust information object (TIO) with said client, said TIO comprising a hash value of a trust entity certificate and associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate;

during an SSL handshake between said client and said server, said server sending a certificate chain that, optionally, contains a root certificate (RC) to said client; and

said client validating said server certificate using said TIO.

8. The method of Claim 7, wherein said client hashes a server certificate and compares a resulting digest against a list of trusted entity certificate thumbprints obtained from said TIO.

9. The method of Claim 8, wherein if a thumbprint match is not found:

said client retrieves an RC from a trusted server;

said client performs certificate chain validation up to a root certificate authority (CA);

once an entire certificate chain is validated, said client tries to validate said CA RC;

wherein, if said RC is included in said certificate chain, said client hashes said RC and looks up said TIO in said client;

wherein if a resulting hash value and a corresponding trust bit are found in said TIO, then said certificate chain is considered to be valid and session initiation proceeds.

10. The method of Claim 8, wherein if a thumbprint match is, said client checks a trust bit vector associated with said certificate to ensure that an authenticated server is trusted in the context of a session being established.

11. The method of Claim 9, wherein if necessary trust capabilities are not set on a matched thumbprint, said client fails a session initiation handshake.

12. The method of Claim 7, wherein a hash value in said TIO is taken by hashing a valid certificate; and wherein said certificate is accepted by a validation mechanism, even when said client receives an expired root certificate.

13. The method of Claim 7, further comprising the step of:

providing in said TIO a designated trust bit associated with a site certificate for identifying a site that is trusted to perform certain operations;

wherein when said client executes a script it checks said certificate and associated trust information; and

wherein if said trust bit indicates that a site identified by its certificate is trusted for an intended operation, then access permission is granted.

14. A method for delivering certificates with associated trust information from a server to a client for verification of a received certificate by said client, comprising the steps of:

embedding a trust information object (TIO) within said client, said TIO comprising a hash value of a trust entity certificate and associated trust information;

said client connecting to said server to determine whether a new TIO is available; and

said server sending a new TIO to said client if there is a more recent TIO.

15. The method of Claim 14, further comprising the step of:

sending a TIO including a signing certificate to said client, wherein trust information of said signing certificate indicates that said certificate can be trusted for signing said TIO.

16. The method of Claim 14, wherein said client fetches said TIO from a trusted server, said client ensuring that a root certificate that signed said signing certificate is contained in said TIO and is not revocable.

17. The method of Claim 14, wherein said client verifies a digital signature of said TIO with a signing certificate, along with a TIO sent to said client.

18. The method of Claim 17, wherein multiple signatures are verified, depending on the number of signatures specified in said TIO; wherein said client hashes said signing certificates one by one; and wherein if proper results are found in said TIO and said certificates are trusted for signing said TIO, then said TIO proves that it was not tampered with.

19. The method of Claim 18, wherein said signing certificates exist in said TIO in said client before said TIO is signed.

20. The method of Claim 14, wherein said TIO is delivered to said client via a broadcast channel;

wherein a provider delivers a TIO to said client that contains a signing certificate and associated trust information by either of including said signing certificate in an initial TIO saved in a client persistent memory, or by sending said TIO to said client through a secure channel before using said broadcast channel.

21. The method of Claim 14, further comprising the step of:

updating said TIO on a per session basis when said TIO is not persistently stored.

22. An apparatus for delivering certificates with associated trust information from a server to a client for verification of a received certificate by said client, comprising:

a trust information object (TIO) associated with said client;

said TIO comprising a hash value of a trust entity certificate and associated trust information.

23. The apparatus of Claim 22, wherein said trust information indicates a level of trust for a trusted entity associated with said TIO.

24. The apparatus of Claim 22, said TIO comprising any of:

a time stamp which indicates a date that said TIO is generated;

a trust attribute that comprises trust information associated with an entity represented by its certificate; and

a thumb print comprising a hash of a public key embedded in a certificate that represents a trusted entity.

25. An apparatus for delivering certificates with associated trust information from a trust information provider to a client for verification of a received certificate by said client, comprising:

a trust information object (TIO) associated with said client; and

a hash value of a trust entity certificate and associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate, said hash value contained within said TIO.

26. The apparatus of Claim 25, wherein said TIO comprises any of:

a trusted entity's certificate;

a trust vector of said trusted entity's certificate;

a value indicating a number of signatures required for a next update;

a date said TIO is created; and

a digital signature of all data including said certificate, trust vector, number of signatures. and timestamp, contained in said TIO.

27. The apparatus of Claim 1 wherein said hash value is determined using any of MD5 and SHA-1.

28. The apparatus of Claim 21, said TIO conforming to the PKCS#7 standard.

29. The apparatus of Claim 1, said TIO comprising a TIO derived from a set of popular root CA certificates hard coded into said client's software.

30. The apparatus of Claim 1, said TIO further comprising:

a copy of said TIO saved in a persistent memory during said client's build time.

31. An apparatus for delivering certificates with associated trust information from a server to a client for verification of a received certificate by said client, comprising:

a trust information object (TIO) associated with said client, said TIO comprising a hash value of a trust entity certificate and associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate;

means for sending a certificate chain from said server that, optionally, contains a root certificate (RC) to said client during an SSL handshake between said client and said server; and

means at said client for validating said server certificate using said TIO.

32. The apparatus of Claim 31, wherein said client hashes a server certificate and compares a resulting digest against a list of trusted entity certificate thumbprints obtained from said TIO.

33. The apparatus of Claim 32, wherein if a thumbprint match is not found:

said client retrieves an RC from a trusted server;

said client performs certificate chain validation up to a root certificate authority (CA);

once an entire certificate chain is validated, said client tries to validate said CA RC;

wherein, if said RC is included in said certificate chain, said client hashes said RC and looks up said TIO in said client;

wherein if a resulting hash value and a corresponding trust bit are found in said TIO, then said certificate chain is considered to be valid and session initiation proceeds.

34. The apparatus of Claim 32, wherein if a thumbprint match is, said client checks a trust bit vector associated with said certificate to ensure that an authenticated server is trusted in the context of a session being established.

35. The apparatus of Claim 34, wherein if necessary trust capabilities are not set on a matched thumbprint, said client fails a session initiation handshake.

36. The apparatus of Claim 31, wherein a hash value in said TIO is taken by hashing a valid certificate; and wherein said certificate is accepted by a validation mechanism, even when said client receives an expired root certificate.

37. The apparatus of Claim 31, further comprising:

a designated trust bit in said TIO associated with a site certificate for identifying a site that is trusted to perform certain operations;

wherein when said client executes a script it checks said certificate and associated trust information; and

wherein if said trust bit indicates that a site identified by its certificate is trusted for an intended operation, then access permission is granted.

38. An apparatus for delivering certificates with associated trust information from a server to a client for verification of a received certificate by said client, comprising:

a trust information object (TIO) embedded within said client, said TIO comprising a hash value of a trust entity certificate and associated trust information;

means associated with said client for connecting to said server to determine whether a new TIO is available; and

means associated with said server for sending a new TIO to said client if there is a more recent TIO.

39. The apparatus of Claim 38, further comprising:

means for sending a TIO including a signing certificate to said client, wherein trust information of said signing certificate indicates that said certificate can be trusted for signing said TIO.

40. The apparatus of Claim 38, wherein said client fetches said TIO from a trusted server, said client ensuring that a root certificate that signed said signing certificate is contained in said TIO and is not revocable.

41. The apparatus of Claim 38, wherein said client verifies a digital signature of said TIO with a signing certificate, along with a TIO sent to said client.

42. The apparatus of Claim 41, wherein multiple signatures are verified, depending on the number of signatures specified in said TIO; wherein said

client hashes said signing certificates one by one; and wherein if proper results are found in said TIO and said certificates are trusted for signing said TIO, then said TIO proves that it was not tampered with.

43. The apparatus of Claim 42, wherein said signing certificates exist in said TIO in said client before said TIO is signed.

44. The apparatus of Claim 38, wherein said TIO is delivered to said client via a broadcast channel;

wherein a provider delivers a TIO to said client that contains a signing certificate and associated trust information by either of including said signing certificate in an initial TIO saved in a client persistent memory, or by sending said TIO to said client through a secure channel before using said broadcast channel.

45. The apparatus of Claim 38, further comprising:

means for updating said TIO on a per session basis when said TIO is not persistently stored.

46. A method for delivering certificates with associated trust information from a server to a client for verification of a received certificate by said client, comprising the steps of:

associating a trust information object (TIO) with said client;

providing within said TIO a hash value of a trust entity certificate and associated trust information.

47. The method of Claim 46, wherein said trust information indicates a level of trust for a trusted entity associated with said TIO.

48. The method of Claim 46, said TIO comprising any of:

a time stamp which indicates a date that said TIO is generated;

a trust attribute that comprises trust information associated with an entity represented by its certificate; and

a thumb print comprising a hash of a public key embedded in a certificate that represents a trusted entity.

49. A method for delivering certificates with associated trust information from a trust information provider to a client for verification of a received certificate by said client, comprising the steps of:

providing a trust information object (TIO) to said client; and

providing as part of said TIO a hash value of a public key embedded in a certificate that represents a trusted entity.